快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- **安全技术** <=
- 业界动态

本类热门
- 如何利用黑客技术跟踪并分析一名目标人物
- 有关无线安全与黑客的话题
- 让我们回归(by 默难)
- 通用ShellCode深入剖析[转]
- Format String 漏洞介绍/总结(一)
- 结合实例解读ELF文件-阅读笔记(1)

信息安全管理

提交文章： 艰苦
提交日期： 2004-05-14
文章属性： 转载
文档类别： 安全技术
浏览次数： 今1次/总2215次

如何评估自有的安全管理状况

安全管理是一个仍在继续发展的领域，除了CC中的系统和产品标准、SSE-CMM中涉及到的系统运行安全管理和BS7799中的如风险管理和涉及安全方面的人员管理等外，企业还应该更加自己的需要制定了相应的安全政策并对此有效的执行。

安全管理的前提是制订保证安全目标的政策。安全政策包括物理方面的政策如关键计算设备的安全政策、逻辑方面的政策如数据访问、安全政策和行政制约方面的安全政策如人员安全管理政策。安全管理的一个重要组成部分是对安全政策实施过程与结果的审计并根据审计结论采取必要的行动，目前虽然对安全管理力度的级别定义在国内的信息系统的等级保护中有了要求，但具体的实施细则还没有正式执行，目前还无法进行参照。不过有一个原则是在高密级要求环境下应采取比低密级更强的安全管理。

我们可以看看BS7799是如何建立一个企业（组织）的安全管理体系的，
BS 7799-2：2002 定义了九个实施步骤或阶段：
第 1 步:定义信息安全管理体系的范围
第 2 步:定义安全方针
第 3 步:确定系统化的风险评估方法
第 4 步:确定风险
第 5 步:评估风险
第 6 步:识别和评价供处理风险的可选措施
第 7 步:选择控制目标和控制措施处理风险
第 8 步:准备适用性声明
第 9 步:管理层批准残余风险

另外也可以参考北京市委办公厅、北京市人民政府办公厅2001发布的《北京市党政机关计算机网络与信息信息安全管理办法》中对信息安全管理的要求，该办法对组织领导和责任制、安全方案审查、安全服务单位、产品资质准入、保密要求和管理制度、监控和应急处理、信息内容、人员上岗培训、宣传、教育、监督检查、法律责任、实施时间等方面都作了不同的要求，应该说涉及面还是很广的。

在进行自评估时，除了可以参照BS7799的控制项进行自我检查外，还可以考虑采用外部的风险评估服务，其目的是通过系统的风险评估识别企业信息系统中的风险点，并区分出高低，例如哪些威胁才是需要关注的，定位出特地的安全需求。并且在一定条件下，指导企业进行最有效的降低总体风险和特定风险，监控不断变化的安全状况，最终指导进行安全风险管理，为企业的安全管理体系的建立提供原始信息。
如何针对安全管理的内容进行管理？

首先，需要根据企业的现实情况，明确大概的安全方针并制定相应的安全策略。在制定策略时需要注意不能脱离实际，很多安全策略和标准实际上是为 一种理想状态下写的，包括一些信息安全顾问偶然也会犯这种错误，并没有真正了解到当前企业的安全需求和现状的

情况下制定的安全策略在企业的实际实施过程中必然会出现问题，管理层或使用者会发现策略的定制者们并未理解他们真正的需要。如果这些安全策略过于理论化或限制性太强，那么企业组织就会漠视这这些策略。因此在安全策略定制必须遵循以下原则：越符合现状越容易推行，越简单越容易操作，改动越小越容易接受.同时，在制定信息安全管理制度时要注意考虑企业现有的文化。许多信息安全方面的规章制度都是参考制度模板或者以其他组织的规章制度为模板而制定出来的。与企业文化和业务活动不相适应的信息安全管理制度往往会导致发生大范围的不遵守现象。另外，规章制度还必须包括适当的监督机制。

其次，要对现有信息系统进行安全评估。信息系统安全评估是指根据公认的标准和指导规范对信息系统及其业务应用的效能、效率、安全性进行监测、评估和控制的过程，以完成企业的安全目标，同时树立风险管理意识并遵循这个进行相关的安全体系建立。

再次，要充分认识到信息安全管理是一个过程。信息安全是一个动态的过程，必须分阶段的对安全策略进行调整，同时安全攻击和防范技术都在高速的发展，而这一切是一个没有终点的过程，必须建立在一套好的信息安全管理机制的基础上。

总的来说，安全管理不是一种即买即用的东西。一购买就能提供足够安全水平的安全管理体系是不存在的。建立一个有效的信息安全管理首先需要要在信息安全评估的基础上，制定出相关的管理策略和规章制度后，才能通过配套选用相应的安全产品搭建起整个信息安全架构。现在有些企业通过安装部分的安全产品或者制定了一些安全制度但没有得到良好的执行，我们也不能认为这个企业就有了信息安全管理体系，因为安全管理体系的建立是一个管理系统的验证规范， 需依循“ PDCA ”循环进行，包括持续改善，订定政策、管理审查、文件管制、内部稽核等。而且信息安全管理与一般管理的不同在于信息安全管理着重在风险评

估及管理，并选择适当控制措施，将组织损失降到最低。风险评估的过程不是一段时间的工作，而是需要随着技术的发展及企业自身的变化持续改善的过程。企业实施了一套信息安全管理体系并不表示其自身信息安全受到绝对的保护，而是确保其本身的信息安全价值、风险等已确实评估，同时为当前信息系统的安全状态提供了一个快照，并在此基础上进行不断的控制与管理。

需要说明的是，要遵循以上要求即使对最有安全意识和执行能力的企业来说也不是一件简单的事，但总体来说提高信息安全管理水平已是一股不可违逆的潮流，所有的机构或企业已不是“ 做 ”与“ 不做 ”的问题，而是必须尽早实施的问题。企业应权衡自身承受安全的风险与成本，订定出一套符合本身需求的安全政策，改善自身的营运体制，以符合国际安全标准与世界潮流。

如何建设一个安全监控中心（SOC）？

虽然信息安全管理问题主要是个从上而下的问题，不能指望通过某一种工具来解决，但良好的安全技术基础架构能有效的推动和保障信息安全管理。随着国内行业IT应用度和信息安全管理水平的不断提高，企业对于安全管理的配套设施如安全监控中心（SOC）的要求也将有大幅度需求，这将会是一个较明显的发展趋势。

推行SOC的另外一个明显的好处是考虑到在国内企业目前的信息化程度下直接实施信息管理变革的困难性，如果尝试先从技术角度入手建立SOC相对来说阻力更小，然后通过SOC再推动相应的管理流程制定和实施，这也未尝不是值得推荐的并且符合国情的建设方式，而且目前已经有些IT应用成熟度较高的大型企业开始进行这方面工作的试点和探索了，因为这些组织已经认识到仅依赖于某些安全产品，不可能有效地保护自己的整体网络安全，信息安全作为一个整体，需要把安全过程中的有关各方如各层次的安全产品、分支机构、运营网络、客户等纳入一个紧密的统一安全管理平台中，才能有效地保障企业的网络安全和保护原有投资，信息安全管理水平的高低不是单一的安全产品的比较，也不是应用安全产品的多少和时间的比较，而是组织的整体的安全管理平台效率间的比较。下面我们就来谈谈建立一个SOC应该从那些方面考虑。

首先，一个较完善的SOC应该具有以下功能模块：

l 安全设备的集中管理
n 统一日志管理（集中监控）：包括各安全设备的安全日志的统一监 控；安全日志的统一存储、查询、分析、过滤和报表生成等功能、安全日志的统一告警平台和统一的自动通知等；

模块分析：大型网络中的不同节点处往往都部署了许多安全产品，起到不同的作用。首先要达到的目标是全面获取网络安全实时状态信息，解决网络安全管理中的透明性问题。解决网络安全的可管理控制性问题。从安全管理员的角度来说，最直接的需求就是在一个统一的界面中可以监视到网络中每个安全产品的运行情况，并对他们产生的日志和报警信息进行统一分析和汇总。
n 统一配置管理（集中管理）：包括各安全设备的安全配置文件的集中管理，提高各管理工具的维护管理水平，提高安全管理工作效率；有条件的情况下实现各安全产品的配置文件（安全策略）的统一分发，修正和更新；配置文件的统一在（离）线管理，定期进行采集和

审核，对安全产品的各种属性和安全策略进行集中的存储、查询。
模块分析：目前企业中主要的安全产品如防火墙、入侵检测和病毒防护等往往是各自为政，有自己独立的体系和控制端。通常管理员需要同时运行多个控制端，这就直接导致了对安全设备统一管理的要求。不过从目前国内的情况来说，各不同厂商的安全产品统一管理的难度较大，统一监控更容易实现，在目前现状中也更为重要。

目前国内现状是各个安全公司都从开发管理自己设备的管理软件入手，先做到以自己设备为中心，把自己设备先管理起来，同时提出自己的协议接口，使产品能够有开放性和兼容性。这些安全设备管理软件和网络管理软件类似，对安全设备的发现和信息读取主要建立在SNMP协议基础上，对特定的信息辅助其他网络协议。获取得内容大部分也和网络设备管理相同，如CPU使用情况，内存使用情况，系统状态，网络流量等。

n 各安全产品和系统的统一协调和处理（协同处理）：协调处理是安全技术的目标，同时也符合我国对信息安全保障的要求即实现多层次的防御体系。整体安全技术体系也应该有多层次的控制体系。不仅仅包含各种安全产品，而且涉及到各主机操作系统、应用软件、路由交换设备等等。
模块分析：目前国内有部分提法是IDS和防火墙的联动就是基于这种思路的，但是实际的使用情况中基本上没有客户认同这点，原因当然有很多，但实际上要实现这点还需要较长的技术积累。
n 设备的自动发现：网络拓扑变化后能自动发现设备的调整并进行基本的探测和给出信息。
模块分析：大部分企业内部的网络的拓扑都是在变化的，如果不支持设备的自动发现，就需要人工方式解决，给管理员造成较大的工作压力，也不能掌握网络的实际拓扑，这样不便于排错和发现安全故障。可以采用自动搜寻拓扑的机制。如IBM Tivoli Netview可以自动发现大多数网络设备的类型，或通过更改MIB库，来随时添加系统能识别的新的设备。

l 安全服务的集中管理
n 实现安全相关软件/补丁安装情况的管理功能，建立安全相关软件/补丁信息库，提供查询、统计、分析功能，提供初步的分发功能。
模块分析：微软在对自己的操作系统的全网补丁分发上走的比较前，成功的产品有SUS和SNS等，国际上也有部分的单一产品是作这个工作的，但目前还没有看到那个SOC集成了这个模块。

n 安全培训管理：建立安全情报中心和知识库（侧重安全预警平台），包括：最新安全知识的收集和共享；最新的漏洞信息和安全技术,；实现安全技术的交流和培训。持续更新发展的知识和信息是维持高水平安全运行的保证。

模块分析：虽然这个模块的技术含量较低，但要为安全管理体系提供有效的支持，这个模块是非常重要的，有效的安全培训和知识共享是提示企业的整体安全管理执行能力的基础工作，也有助于形成组织内部统一有效的安全信息传输通道，建立安全问题上报、安全公告下发、处理和解决反馈的沟通平台。

n 风险分析自动化：自动的搜集系统漏洞信息、对信息系统进行入侵检测和预警，分析安全风险，并通过系统安全软件统一完成信息系统的补丁加载，病毒代码更新等工作，有效的提高安全工作效率，减小网络安全的"时间窗口"，大大提高系统的防护能力。

模块分析：安全管理软件实施的前提是已经部署了较完善的安全产品，如防火墙，防病毒，入侵检测等。有了安全产品才能够管理和监视，安全管理平台的作用在于在现有各种产品的基础上进行一定的数据分析和部分事件关联工作，例如设置扫描器定期对网络进行扫描，配合该时间段的入侵检测系统监控日志和补丁更新日志，就可以对整网的技术脆弱性有个初步的了解。

l 业务流程的安全管理
n 初步的资产管理（资产、人员）：统一管理信息资产，汇总安全评估结果，建立风险管理模型。提供重要资产所面临的风险值、相应的威胁、脆弱性的查询、统计、分析功能。

模块分析：国内外安全厂商中资产管理功能都很简单，和现有的财务、运营软件相差非常大，基本上是照般了BS7799中的对资产的分析和管理模块。

n 安全管理系统与网管系统的联动（协调处理）：安全管理系统和网络管理平台已经组织常用的运营支持系统结合起来，更有效的利用系统和人力资源，提高整体的运营和管理水平。

模块分析：如果可能的话，由于各产品的作用体现在网络中的不同方面，统一的安全管理平台必然要求对网络中部署的安全设备和部分运营设备的安全模块进行协同管理，这也是安全管理平台追求的最高目标。但这并非是一个单纯的技术问题，还涉及到行业内的标准和联盟。目前在这方面作的一些工作如 Check Point公司提出的opsec开放平台标准，即入侵检测产品发现攻击和check point防火墙之间的协调，现在流行的IPS概念，自动封锁攻击来源等，都在这方面作了较好的尝试，在和整体的网络管理平台的结合方面，目前国内外作的工作都较少，相对来说一些大型的IT厂商如IBM/CISCO/CA由于本身就具备多条产品线（网络、安全、应用产品），其自身产品的融合工作可能已经作了一些，但总体来说成熟度不高。

n 与其它信息系统的高度融合：实现与OA、ERP等其他信息系统的有机融合，有效的利用维护、管理、财务等各方面信息提高安全管理水平。安全管理的决策分析和知识经验将成为公司管理的重要组成部分。
l 组织的安全管理
n 组织构成：根据企业的不同情况建立专职或兼职的安全队伍，从事具体的安全工作。由于信息安全工作往往需要多个业务部门的共同参与，为迅速解决业务中出现的问题，提高工作效率，公司必须建立跨部门的协调机制。具体协调机构应由专门的安全组织负责，并明确牵头责任部门或人员。有条件的企业或者组织应成立独立的安全工作组织。
n 组织责任：
a) 建立健全相关的安全岗位及职责；
b) 制定并发布相关安全管理体系，定期进行修正；
c) 对信息系统进行安全评估和实施，处理信息安全事故；
f) 部门间的协调和分派并落实信息安全工作中各部门的职责；
以上是SOC必须具备的一些模块，现阶段国内外也有一些厂商推出了安全管理平台软件，从推动整个行业发展来看当然是好现象，但萝卜快了不洗泥，其中也存在一些发展中的问题，比如作为一个SOC必然要求具备统一的安全日志审计功能，但单一安全设备审计软件不能等同于安全管理平台，究其原因为国内现有安全厂商中安全设备厂商占多数，优势项目是在已有安全设备上添加统一日志管理和分析功能，由于是单个厂商的行为缺乏整体的行业标准，导致目前的安全审计软件普遍缺乏联动性，不支持异构设备，就算是对java的支持各个厂商的实现力度也不同，普遍只具备信息统计功能和分析报告的功能。。
在目前的安全管理平台提供商中，能提供完整的产品体系厂商非常少。而号称专业的安全产品厂商，因为安全产业起步很晚，这些厂商只能在某个领域做深，还无法提供整套的安全产品线，这也是一个现实。作为用户应该认清需求，把各种安全产品在自己网络中结合起来，深入了解安全管理平台提供商的实力，才能够达到安全目的，满足自己的安全需求。
最后，从投入产出比的角度来说，因为SOC往往只是一个软件平台的开发工作，大多数情况下不需要或者较少需要新的硬件投入，总投入往往不是很大，如果上了SOC后即使不能完善和推荐安全管理体系，也可以起到减轻管理员的工作负担，增强管理员的控制力度，并对整个网络内的安全状况进行统一监控和管理的作用，这样总体来说安全管理平台SOC的投入产出就非常值得。

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net